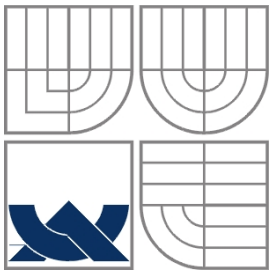
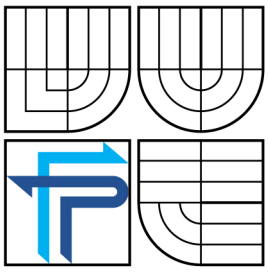


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH BEZPEČNOSTNÍ POLITIKY IS/IT PODNIKU

DRAFT OF COMPANY IS/IT SECURITY POLICY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

OTA KULIŠ

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. VIKTOR ONDRÁK, Ph.D.

BRNO 2008

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2007/08
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Kuliš Ota

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Návrh bezpečnostní politiky IS/IT podniku.

v anglickém jazyce:

Draft of company IS/IT security policy.

Pokyny pro vypracování:

Úvod
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

Bezpečností politika IS: sborník příspěvků ke konferenci pořádané u příležitosti 10. výročí založení společnosti EUNIS-CZ. 1. vyd. Plzeň : Západočeská univerzita, 2007 -- 76 s. ISBN: 978 80-7043-554-0 (brož.)
ČSN 36 9789 - ČSN ISO/IEC 15408 1-3. Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
ČSN EN ISO 27001. Systémy managementu bezpečnosti informací - specifikace s návodem pro použití. Praha: Český normalizační institut, 2005
ČSN ISO/IEC TR 13335. Informační technologie - Směrnice pro řízení bezpečnosti IT. Praha: Český normalizační institut, 1996.
DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Computer Press 2004, ISBN 80-251-0106-1
HANÁČEK, P. – SAUDEK, J. Bezpečnost informačních systémů, ÚSIS, Praha, 2000, 127 s. ISBN 80-238-5400-3
HORÁK, J. Bezpečnost malých počítačových sítí. Grada. 2003. ISBN 80-247-0663-6
PROSISE, C., MANDIA,K. Počítačový útok Detekce, obrana a okamžitá náprava. Computer Press. ISBN 80-7226682-9

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2007/08.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská
L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. Ing. Miloš Koch, CSc.
Děkan fakulty

V Brně, dne 15.2.2008

Abstrakt

Tato bakalářská práce analyzuje problematiku bezpečnosti IS/IT v reálném prostředí středně velké české firmy a navrhuje řešení této problematiky a jeho praktickou implementaci. Vzhledem k rozsahu problematiky bezpečnosti je práce soustředěna na bezpečnostní politiku firmy.

Abstract

The presented bachelor's thesis analyses problems of IS/IT security in the factual environment of a middle-sized Czech company and suggests a solution to these problems and its practical implementation. Taking into account the scope of security issues, the thesis is focused on the company security policy.

Klíčová slova

bezpečnost, bezpečnostní politika, bezpečnostní směrnice, bezpečnost dat, bezpečnostní normy, management bezpečnosti, zálohování dat

Key words

security, security policy, security guidelines, data security, security standards, security management, data backup

Bibliografická citace

KULIŠ, O. *Návrh bezpečnostní politiky IS/IT podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2008. 62 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Prohlášení autora o původnosti práce

Prohlašuji, že jsem předloženou bakalářskou práci zpracoval samostatně a pod vedením svého vedoucího bakalářské práce. Prohlašuji, že citace použitých pramenů je úplná a příslušné prameny uvádím v literatuře.

V Brně, dne 26. května 2008 .....

Podpis

Poděkování

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Viktoru Ondrákovi, Ph.D. za vstřícný přístup, užitečné rady a odbornou pomoc při zpracování bakalářské práce.

Obsah

1 Úvod a cíl práce

1.1 Úvod

Informační technologie dnes pronikají i na místa, kde bychom si je před pár lety nedovedli vůbec představit. Jedná se o dlouhodobý trend. Téměř ve všech organizacích od státní správy až po privátní sektor se zpracovává narůstající množství dat. Vlastnit správnou informaci ve správný čas může znamenat značnou konkurenční výhodu a stejně tak může nesprávné zacházení s informací mít devastující účinky pro organizaci.

S rostoucím významem informačních technologií pro zpracování dat roste i množství a profesionalita útoků na ně. Informace považujeme za aktiva a je v zájmu každé organizace si svá aktiva chránit. Narušení informačních systémů obchodních společností, finančních institucí, institucí státní správy a dalších organizací může znamenat ochromení chodu těchto organizací. Proto je potřebné zavést určitá pravidla, která jasně popisují co je předmětem ochrany, co je potřebné pro ochranu udělat a v neposlední řadě také odpovědnosti a kontrolu. Tato pravidla a zásady představují základ pro zajištění informační bezpečnosti a nazývají se informační bezpečnostní politika. Oblast zabezpečení IT je tak obsáhlá, že jsem se při řešení bakalářské práce omezil právě na bezpečnostní politiku a její organizační zajištění.

V první části práce analyzuji současný stav informačních technologií v konkrétní firmě. Z důvodu citlivosti zde uváděných údajů si tato firma nepřeje být jmenována a bude uváděna pod názvem XYZ s.r.o.

V druhé části se zabývám teoretickými východisky a aktuálním stavem vědění v oblasti informační bezpečnosti.

Třetí část sestává z návrhu řešení současného stavu. Je zde uveden návrh na bezpečnostní cíl a strategii firmy a organizační zajištění bezpečnosti ve firmě.

1.2 Cíl práce

Cílem mé práce je na základě provedené analýzy odhalit problémová místa dosavadní bezpečnostní politiky konkrétní firmy a poté vznést návrh na bezpečnostní cíl, strategii a organizační zajištění bezpečnosti ve firmě. Součástí řešení je návrh na vytvoření bezpečnostních směrnic pro oblasti fyzické bezpečnosti a bezpečnosti prostředí, klasifikace a ochrany uložených dat, ochrany logického přístupu k datům, ochrany dat přenášených počítačovou sítí, ochrany dat před zničením a personální bezpečnosti.

2 Analýza současného stavu

2.1 Informace o firmě

Firma, ve které jsem bakalářskou práci zpracovával, si nepřeje být jmenována z důvodu citlivosti zde uváděných údajů. V práci bude tato firma uváděna pod názvem XYZ s.r.o.. Neuvedení názvu firmy nebude mít žádný vliv na řešení problematiky bezpečnosti.

Firma XYZ s.r.o. se zabývá obchodní činností v oblasti stavebních hmot a barev v České republice od roku 1994. Vlastníkem je rakouská společnost, která v ní má 100% podíl a je součástí nadnárodního koncernu. Obchodní výsledek v podobě trvalého růstu společnosti v průměru o 15% ročně za období od roku 1997 do 2007 poukazuje na rostoucí podíl na trhu a rostoucí zájem o výrobky společnosti. Tržní podíl na českém trhu představuje přibližně 7%.

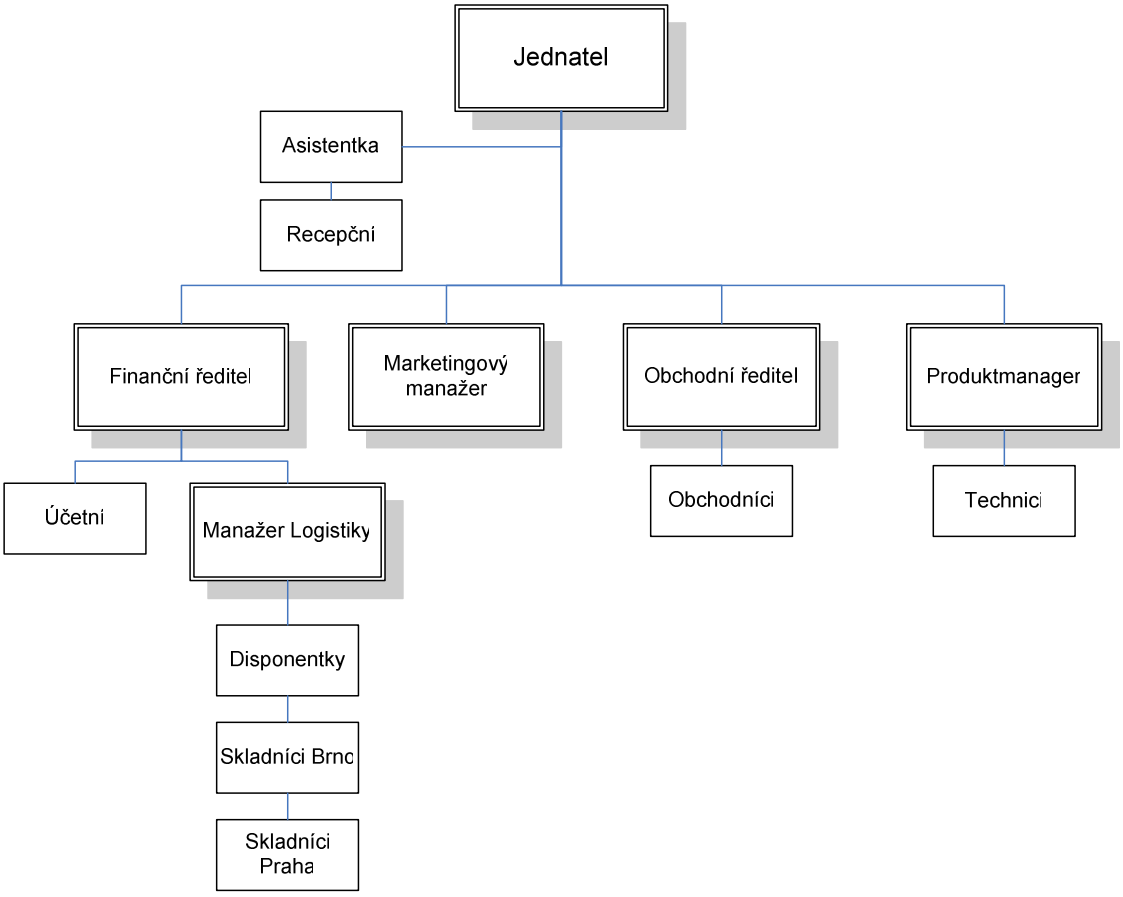
Centrála a ústřední sklad jsou umístěny na okraji města Brna. Druhý sklad firmy je umístěn v Praze. V Brně je soustředěno klíčové počítačové vybavení a data. Prakticky denně přichází všichni zaměstnanci společnosti do styku s informačními technologiemi. K firemním datům přistupují buď vzdáleně nebo v místě pracoviště.

Firma nemá žádného vyčleněného pracovníka pro informační technologie a jejich provoz je zajištěn externí firmou na bázi outsourcingu. Prostředníkem mezi správcem IT a firmou jsou vedoucí finančního oddělení a jednatel.

2.2 Organizační struktura firmy

Organizační struktura firmy je funkcionální, jejímž hlavním znakem je logické seskupování funkcí (činností). Výhody této struktury jsou jednoduchost, specializace a efektivní dělba práce.

Firma má 6 řídících pracovníků a největší podíl na počtu zaměstnanců tvoří obchodně techničtí poradci. Celkový počet stálých zaměstnanců je 40 a toto číslo se neustále zvyšuje s růstem společnosti.



Obrázek 1: Organizační struktura firmy

2.3 Počítačová síť

Firemní síť v rámci centrální budovy je realizovaná jako kombinace místní LAN a WLAN. Do sítě jsou připojeny servery a pracovní stanice umístěné v kancelářích a dále se do ní připojují obchodně techničtí poradci se svými notebooky přes bezdrátovou síť. V pražském skladu je umístěna jedna klientská stanice se vzdáleným přístupem do informačního systému přes zabezpečenou VPN. Firma je připojena do sítě internet přes ADSL modem.

2.3.1 Místní síť LAN

Připojení komunikujících uzlů v LAN je realizováno hvězdicovou topologií. Toto zapojení má tu výhodu, že při selhání jedné stanice či kabelu mohou ostatní stanice vysílat a přijímat i nadále. V budově je implementována lokální síť typu Ethernet verze Fast Ethernet, 100Base-TX s přenosovou rychlostí 100Mb/s. Kabeláž použitá

v Ethernetové síti je nestíněná kroucená dvoulinka UTP Cat5e s PVC pláštěm zakončená konektory RJ-45. Kabelové rozvody vedené ze serverovny po budově jsou umístěny v lištách a jsou provedeny správně co se týče dodržování poloměrů ohybu v rozích a tahového zatížení. Zásuvky pro připojení do LAN jsou rozmístěny ve všech kancelářích a zasedacích místnostech a jejich počet v jednotlivých místnostech převyšuje počet pevně připojených pracovních stanic, aby bylo možné připojit další zařízení jako například notebooky nebo síťové tiskárny. Aktivní prvky sítě jsou umístěny do 19“ palcové RACK skříně a jsou to switche od výrobce 3Com a router Cisco zapojený před modemem.

2.3.2 Bezdrátová síť WLAN

Bezdrátové připojení je realizováno přes Wi-Fi access point, který signálem pokrývá hlavní halu centrály, zasedací místnosti a kanceláře. Tato součást sítě je koncipována dle specifikace 802.11b/g standardu Wi-Fi, provozovaná v bezlicenčním pásmu 2,4 Ghz.

Přístupový bod pracuje v roli Access Point/Router a využívá službu filtrování MAC adres, čímž je přístup povolen jen konkrétním zařízením. Pro přístupový bod je vypnut broadcast identifikátoru SSID, takže síť je skrytá. Vysílací výkon je nastaven tak, aby síla signálu vyzařovaného mimo prostory firmy byla minimální. Jako reakce na slabiny technologií WEP a WPA je bezdrátová sít chráněna zabezpečením WPA2 používající šifrovací algoritmus CCMP založený na AES, který je považován za zcela bezpečný.

Bezdrátové připojení do sítě v budově je určeno převážně obchodníkům, kteří nepoužívají stolní PC, ale notebooky, a řídícím pracovníkům, kteří užívají notebook souběžně s pracovní stanicí. Nespornou výhodou bezdrátového připojení je, že není nutno instalovat kabeláž a je možné přenášet zařízení v oblasti pokryté signálem. Osoby připojující se do bezdrátové sítě mají přidělené jméno a heslo, pod kterým se přihlašují. Není ovšem vytvořena směrnice pro používání bezdrátové sítě.

2.3.3 Virtuální privátní síť VPN

Do firemní sítě je umožněn vzdálený přístup řídícím pracovníkům, obchodníkům a pražskému skladu pomocí zabezpečené virtuální privátní sítě VPN. Díky síťovému tunelování je možné prostřednictvím běžného internetového připojení vytvořit virtuální

linku mezi koncovým počítačem a VPN serverem, který navazuje další síťová připojení. VPN server běží na Linuxovém firewallu a je zabezpečen protokolem IPsec (IP security). Uživatelé využívající VPN mají nainstalovaného VPN klienta, připojují se na firemní IP adresu a zadávají své uživatelské jméno a heslo.

2.3.4 Firewall

Zabezpečit síť má před útoky z internetu za úkol firewall na platformě SuSE Linux. Je pro něj použit starší značkový počítač od výrobce Fujitsu-Siemens. Firma má 8 veřejných IP adres. Pro potřeby společnosti jsou nastaveny pravidla a povoleny porty pro služby: SMTP, POP3, IMAP, HTTP, HTTPS, RDP, IPsec. O obsluhu a nastavení firewallu se stará externí správce IT.

2.4 Hardware ve firmě

Firma používá výhradně hardware kompatibilní s operačním systémem Microsoft Windows. Hardwarové vybavení firmy prochází průběžnou obměnou a průměrné stáří stanic a serverů je 1-2 roky.

2.4.1 Servery

Firemní síť je řízena jedním primárním a jedním záložním doménovým řadičem, které hrají roli autentizačního serveru a využívají Microsoft Active Directory. Jedná se o dva servery značky LYNX na platformě Intel s výkonnými dvoujádrovými procesory Intel Xeon. Tyto servery disponují dostatečnou výkonovou rezervou a vyhovují současným i budoucím požadavkům na provoz. Server S1, zajišťuje provoz Microsoft Exchange Server 2007 a slouží jako DNS sever a DHCP server. Server S2 slouží jako fileserver, centrální server pro antivirový program AVG a aplikační a databázový server pro informační systém ABRA G3. Na fileserveru jsou uložena sdílená firemní data poměrně citlivé povahy a data jednotlivých uživatelů z důvodu centralizovaného zálohování. Třetí server pracuje pro potřebu kamerového systému jako videoserver a žádné jiné služby neposkytuje. Jeho hardware odpovídá výkonnější pracovní stanici. Jsou na něj přes digitalizační kartu připojeny analogové kamery, které sledují venkovní prostory budovy a skladu.

Pro zvýšení bezpečnosti je vytvořena demilitarizovaná zóna DMZ, kde jsou servery chráněny jak před útoky zvenčí, tak i zevnitř. Servery jsou pod 24 hodinovým dohledem externího správce IT služeb. Běžnou správu a kontrolu systému serverů provádí pracovník externího správce IT využitím zabezpečeného internetového připojení, takzvanou vzdálenou správou. Události o veškerých službách běžících na serverech a stavu hardware jsou interně monitorovány a v případě poruchy je automaticky vyrozuměno servisní středisko, odkud je možné dálkovou správou poruchu odstranit.

Všechny servery mají vlastní záložní zdroj elektrické energie UPS. Při výpadku napájení jsou servery schopny přibližně třiceti minut bezpečného chodu. Servery jsou nastaveny tak, aby při přerušení dodávky elektrické energie bezpečně ukončily svoji činnost.

2.4.2 Klientské stanice

Klientské stanice jsou běžná PC značky LYNX určená pro kancelářskou práci. Typická konfigurace obsahuje procesor AMD, dostatečnou kapacitu operační paměti RAM a optickou mechanikou CD/RW nebo DVD/RW. Na všech klientských stanicích jsou nainstalovány síťové karty pro 10/100Mb Ethernet. Ve firmě je podporováno používání USB flash disků a proto mají všechny počítače vyvedeny USB konektory na předním panelu. Vybrané stanice jsou napojeny na záložní zdroj elektrické energie UPS z důvodu zamezení ztráty neuložené práce.

Pracovní stanice jsou průběžně, ale ne pravidelně, podrobovány profylaxi (vyčištění od prachu) ve snaze zamezit snižování jejich životnosti a minimalizovat náklady spojené s opravou a nákupem náhradních dílů.

2.4.3 Notebooky a mobilní zařízení

Přenosné počítače se ve firmě využívají z důvodu mobility. Typický firemní notebook je vybaven Wi-Fi kartou, síťovou kartou a USB porty. Konfigurace je postačující pro provoz Windows XP a firemních aplikací.

Notebooky obchodníků nejsou majetkem firmy, ale ta jim vyplácí paušální příspěvek na jejich provoz. Jejich průběžnou správu zajišťuje externí správce IT, který si s nimi po telefonu domlouvá schůzky v Brně. Notebooky, stejně jako ostatní firemní

počítače jsou určeny pro práci, ale vzhledem k jejich povaze se kontrola toho kdo a jak s nimi pracuje prakticky nevykonává, ani za to není nikdo zodpovědný.

Spolu s notebooky používá téměř každý zaměstnanec firemní mobilní telefon. Jedná se o přístroje značky Nokia určené pro firemní klientelu. Management a obchodníci používají sofistikované „chytré telefony“ s podporou operačního systému Symbian. Tyto přístroje jsou například schopny komunikace přes bezdrátové sítě WiFi, prohlížení webových stránek či firemních dokumentů a mají vestavěného e-mailového klienta. Jsou, co se funkčnosti týče, schopny v určitých ohledech nahradit PDA či notebooky. Jejich zabudovaná paměť společně s paměťovou kartou může poskytnout několik gigabajtů pro ukládání dat. V současnosti jsou ve firmě považovány pouze za „telefony“ určené k uskutečňování hovorů, i když větší část zaměstnanců využívá jejich pokročilých funkcí.

2.5 Software ve firmě

Ve firmě se software rozlišuje na operační systémy, aplikace a antivir/antispam.

2.5.1 Operační systémy

Ve firmě se výhradně používají operační systémy Microsoft Windows. Výjimkou je instalace SuSe Linuxu na firewallu. Servery pracují pod Windows Server 2003. Na všech klientských stanicích je nainstalován operační systém Windows XP Professional s aktualizací Service Pack 2 a záplatami, které jsou stahovány serverem z webu Windows Update a poté distribuovány po síti jednotlivým stanicím.

2.5.2 Aplikační software

Firma využívá hlavně kancelářský balík Microsoft Office a informační systém ABRA G3.

Kancelářský balík Microsoft Office je verze 2003 a na záplaty pro něj není kladen takový důraz jako pro Windows. Jako poštovní klient je využíván Microsoft Outlook 2003 a zaměstnanci mají také možnost přístupu k jejich poštovní schránce přes webové rozhraní Web Access.

Informační systém ABRA G3 je modulární systém, který postačuje pro potřeby firmy střední velikosti. O data se stará server Firebird, který je dostatečně výkonný a zároveň zdarma. Informační systém je aktualizován tak, aby vždy pracoval s platnou legislativou. Každý zaměstnanec podle své funkce pracuje s příslušnými moduly a každá změna dokladů a údajů je zaznamenávaná s časem, kdy k ní došlo, a s identifikací autora a stanice.

Pro prohlížení internetových stránek je používán webový prohlížeč Internet Explorer 6. Má nainstalovány poslední záplaty a z hlediska zabezpečení a zón je správně nastaven.

Vzhledem k tomu, že uživatelé mají práva lokálního administrátora, instalují na stanice i freeware a shareware programy, které stahují z internetu. Existuje ovšem nepsané pravidlo zákazu instalovat software bez dohledu technika od správce IT, ale není to nijak kontrolováno a nejsou stanoveny postihy.

2.5.3 Antivirové a antispamové řešení

Firma využívá komplexní antivirovou ochranu od společnosti Grisoft. O antivirovou ochranu na serverech se stará AVG Network Edition. Tato instalace je centrální instalací AVG a umožňuje spravovat všechny klientské stanice v síti a distribuuje jim aktualizace. Exchange Server využívá pro kontrolu příchozí a odchozí pošty instalaci AVG Email Server Edition. Na pracovních stanicích kontroluje AVG v pozadí veškerou činnost a není povoleno ho vypínat. Některé stanice mají nainstalovaný antispyware SpyBot Search & Destroy či jiný, ale s neaktualizovanými definičními soubory.

Firma pro zamezení spamu využívá řešení zabudované v MS Exchange 2007. Je zde možnost filtrovat podle IP adres, příjemců a odesílatelů. Antispam využívá databáze známých spamových domén a klientská aplikace MS Outlook 2003 využívá svého spamového filtru. Do poštovních schránek se dostává minimální množství spamu.

2.6 Typy zpracovávaných dat

Ve firmě se pohybuje množství různě citlivých dat, která v ní vznikají, obíhají, zanikají, archivují a zálohují se. V současné době není vytvořena koncepce klasifikace

typů zpracovávaných dat. Na souborovém serveru není vytvořena adresářová struktura, která by data dělila podle jejich citlivosti, ale spíše podle oblasti jejich vzniku a to je zásadní rozdíl. Zaměstnanec může přistupovat k takovým datům, která jsou nezbytná pro jeho práci, ale také k datům ke kterým přístup zakázán vyloženě nemá. V současnosti zachází typický zaměstnanec se všemi daty rovnocenně a s nadsázkou by se dalo říci, že se řídí rčením „data jako data“. Zaměřil jsem se na výčet typů dat, které se ve firmě vyskytují, a dále jsem analyzoval kdo pracuje s jakými daty.

Z pohledu citlivosti se ve firmě vyskytují následující typy dat (seřazeno podle hodnoty, kterou mají pro firmu):

- databáze firemního účetnictví (fakturace, majetek, platební styky, atd.)
- databáze pro personalistiku a mzdy
- dokumentace firemních plánů a strategií
- databáze odběratelů a dodavatelů s údaji o jejich obchodní historii, slevách, kontaktech, smluvních podmínkách, atd.
- databáze produktů firmy a technické listy
- dokumenty interních podnikových směrnic a předpisů
- dokumenty a analýzy o konkurenci
- databáze elektronické pošty a do ní vložených souborů příloh
- systémové zálohy
- záznamy z kamerového systému
- fotografie z akcí
- volně šiřitelné dokumenty (reklamní materiály, obsah www stránek)

Vybraná data (adresáře) na fileserveru a jejich typičtí uživatelé:

Finanční oddělení**:** plány a strategie, směrnice, výprodej, zápůjčky firemních aut

Obchodní oddělení**:** zákazníci, obchodníci, nabídky, konkurence, plány, obchodní podmínky, fotky z akcí

Marketingové oddělení**:** reklama, plány a strategie, obsah www stránek

Produktové oddělení**:** technické listy, výrobky

2.7 Zálohování

Vzhledem k velikosti firmy není množství dat tak obrovské, aby se nedalo zálohovat běžnými prostředky. Forma zálohování je různorodá: některá data se zálohují na páskové mechanice, na interních pevných discích nebo na přenosná média a některá se nezálohují vůbec. Prioritu při zálohování dostávají účetní data.

Za nejcennější data se považuje účetní a ekonomická databáze informačního systému ABRA uložená na serveru S2. Tento server je zabezpečen proti selhání pevných disků uspořádáním dvou disků do pole RAID 1. Data ABRY se zálohují společně s ostatními vybranými firemními daty fileserveru každý den přes noc na páskovou mechaniku, kde se každý den přehrává páska, na kterou bylo zálohováno týden předtím. Tudíž je k dispozici záloha této databáze a souborů 7 dní zpět po jednotlivých dnech. Mechanika podporuje funkci autoloader a tak se o výměnu pásek stará sama a není nutné je manuálně vyměňovat každý den. Tato zálohovaná data zahrnují i data považovaná za „archivní“ a tak je archivace a zálohování ve firmě považováno za totéž. Poštovní server má jako ochranu disků uspořádání do pole RAID 5. Během nočních hodin se provádí záloha pošty, která ovšem zůstává na discích serveru. Data videoserveru se nijak nezálohují ani nearchivují. Jeho jediný pevný disk má kapacitu 200 GB a při dosažení určité hodnoty zaplnění disku se naposled uložený videosoubor smaže a nahrazuje se čerstvějším. Záloha systémů serverů a jejich nastavení, která umožňuje obnovit systém po havárii co nejdříve je odpovědností externího administrátora. Neexistuje ale předpis, který by tuto situaci popisoval.

Pracovní stanice zapojené v síti mají vytvořeny zálohy systému (image), s jednou kopií, pro rychlé obnovení. Tyto zálohy má administrátor uloženy ve své firmě. Uživatelé jsou vyzýváni ukládat pracovní data na svůj síťový disk z důvodu centralizovaného zálohování. Je zakázáno ukládat data na systémový disk C z důvodu možné reinstalace systému a tak si mohou data ukládat lokálně na disk D. Nedůvěra

zaměstnanců k systému zálohování ve firmě vede k tomu, že si zálohují svoji práci na USB flash disky. Není ovšem známo, jaká data a v jakém rozsahu si zaměstnanci na flash disky zálohují a zda porušují zákaz vynášet zálohy mimo firemní prostory.

Politika zálohování ve firmě je poněkud nepropracovaná. Není vytvořen plán pro kontrolu záloh. Nejsou vytvořeny psané zálohovací harmonogramy, ale je pouze jeden, který je nepsaný a proměnlivý. Kontrolou správné funkce zálohovací mechaniky je sice pověřen konkrétní zaměstnanec, ale prakticky ji provádí několik lidí podle domluvy, aniž by měli přiřazeny určité role. Záložní kopie jsou skladovány chaoticky, neexistuje jejich jednotná evidence ani evidence místa jejich skladování. Zálohy kritických dat jsou skladovány v serverovně a zbytek je rozmístěn po kancelářích na různých médiích od CD/DVD po flash disky. Předpokládá se, že všechny zálohy zůstávají v budově firmy a je zakázáno je z budovy vynášet.

2.8 Fyzické zabezpečení

Veškerá data a IT vybavení firmy je umístěno v brněnské centrále spojené se skladem, v pronajatém pražském skladu a také je třeba přičíst přenosné počítače obchodníků a dalších zaměstnanců, které jsou v pohybu po celé ČR.

Centrála a hlavní sklad sídlí na neobydleném úseku na okraji města. Sousedí s pneuservisem a jinak je obklopena nevyužitými pozemky. Budova má 2 patra s kancelářemi a celkově je velice rozlehlá vzhledem k velikosti přistavěného skladu. Střeží ji 4 analogové kamery napojené na videoserver. Tyto kamery nejsou schopny zabírat všechny prostory okolo tak rozsáhlé budovy a navíc mají příliš nekvalitní rozlišení na to, aby bylo ze záznamu poznat například obličej člověka nebo SPZ automobilu. Za těchto okolností se kamerový systém dá označit jako zastaralý a nevyhovující. Budova má dva vchody, jeden z hlavního parkoviště pro zaměstnance a zákazníky, druhý z parkoviště při skladu za bránou areálu. Oba vchody ústí u recepce, kde sedí recepční. Recepční má mimo jiné za úkol zabránit nepovolaným osobám ve vstupu do budovy. Všechny návštěvy se musí hlásit na recepci a musí vyčkat do příchodu vyžádaného zaměstnance dolů na recepci. Za ostrahu objektu je zodpovědná najatá externí firma, která je vzdáleně upozorněna při spuštění alarmu zabezpečovacího systému.

Zaměstnanci mají čipové karty, kterými si označují pouze čas příchodu a odchodu z práce. Klíče od kanceláří má na starosti recepční a uchovává je na recepci, odkud si je zaměstnanci ráno vyzvedávají a po skončení pracovní doby zase odevzdávají s tím, že jejich kancelář je zamčená. Tři vedoucí zaměstnanci vlastní master klíč pro celou budovu a klíč od serverovny, kterým disponuje také správce IT. Jediný další člověk, který má přístup do všech prostor, mimo serverovny, je uklizečka.

Místnost s hlavním počítačovým vybavením, serverovna, se nachází v přízemí budovy. Jsou v ní uloženy všechny tři servery, firewall, switche, zálohovací mechanika, telefonní ústředna a další IT zařízení včetně některých náhradních nebo vyřazených dílů. Uspořádání serverů a ostatního vybavení je uspokojující z hlediska rozmístění a okolního prostoru. Po dřívějších problémech s teplotou místnosti je nyní klimatizována výkonným zařízením a teplota je těsně pod 20°C, což má za důsledek vyšší stabilitu provozovaných zařízení a jejich delší životnost. Vchodové dveře do serverovny jsou dřevěné s chybějící skleněnou výplní, jež je nahrazena polystyrenovým plátem zasazeným a přibitým hřebíky do dveří. Toto opatření zcela popírá existenci dveří místnosti a jako protipožární ochrana taktéž nedostačuje. Velká část licencí k firemnímu software a také záloh je umístěna v serverovně v malém trezoru, ve kterém je zasunut jeho klíč, a tedy jako by byl bez ochrany. Další místnost, která obsahuje zálohy a vyřazené pracovní stanice, je místnost zvaná „archiv“.

2.9 Povědomí zaměstnanců o bezpečnosti

Po pohovoru s několika zaměstnanci mohu usoudit, že povědomí zaměstnanců firmy o informační bezpečnosti je průměrné až nízké. Jako důvod tohoto stavu lze označit téměř nulové vzdělávání zaměstnanců o bezpečnosti ve firmě. Jediné „školení“, které zaměstnanci absolvovali bylo přijetí (jako e-mailové přílohy) stručného dokumentu s návrhem firemní směrnice o používání IT.

Těch několik málo bezpečnostních zásad, které by měli nebo musejí praktikovat považují za nedůležité. To, že musejí měnit svá hesla jednou za 30 dní považují za zbytečnost a nechápou důvod pro silná hesla. V tomto případě obcházejí povinnost měnit hesla střídáním stejných hesel pořád dokola v kombinaci se zaznamenáváním svých hesel do mobilních telefonů a papírků uchovávaných na pracovišti. Jak již bylo

řečeno, zaměstnanci si nedávají příliš práce s rozlišováním dat podle jejich citlivosti. Neuvědomují si nebezpečí opuštění pracoviště s přihlášeným počítačem a mnoho dalších nebezpečí. Zaměstnanci se spíše obávají napomenutí za využívání počítačů k osobním účelům. Ve firmě nejsou stanovena pravidla, podle kterých by zaměstnanci byli ve firmě penalizováni za jednání proti základním zásadám bezpečnosti, ani osoba, která by to kontrolovala.

2.10 Současná bezpečnostní politika

V současné době je hlavním požadavkem na externího správce IT, aby zabezpečil podnikovou síť proti virům a útoku zvenčí. Správce poskytl návrh směrnic pro užívání informačních technologií ve firmě. Tyto směrnice jsou velmi stručné, nebyly poskytnuty zaměstnancům k podepsání a slouží spíše jako návod pro počítačově méně gramotné uživatele. Pravidla v nich uvedená jsou považována za „nepsaná“. V zásadě zmiňují následující pokyny:

- Tvorba hesel (délka, tvorba silného hesla, manipulace s heslem)
- E-mail (spam, přílohy, správa schránky)
- Správa dokumentů (ukládání, tvorba názvů, práce ve sdílené složce)
- Zálohování (kam se ve firmě zálohuje, práce se zálohovací mechanikou)
- Kontakt na technika

Mimo již zmíněnou směrnici neexistuje ve firmě jiný dokument zaměřený na bezpečnost. Tento jediný dokument se nevěnuje funkcím a odpovědnostem za řízení bezpečnosti, ale pouze určuje zaměstnance zodpovědného za kontrolu správné funkce zálohovací mechaniky. Oblasti informační bezpečnosti, které nejsou pokryty ve firemní směrnici ani jiném dokumentu jsou: zabezpečení fyzického přístupu, klasifikace firemních dat, bezpečnost lidských zdrojů a problematika zálohování je řešena příliš stručně. Představitelé firmy mají zájem řešit problematiku bezpečnosti podrobněji a věnovat jí více pozornosti.

3 Teoretická východiska

Oblast bezpečnosti informačních technologií prochází rychlým vývojem a neustálými změnami. Současně s tím se mění předpisy pro její řešení. Je nad rámec této práce popisovat všechno dosavadní vědění o informační bezpečnosti. Proto se budu v této části zabývat hlavně základní terminologií, metodami a teoretickými poznatky, kterými je nutné se při řešení bezpečnosti řídit.

3.1 Základní pojmy počítačové bezpečnosti

Pro lepší pochopení problematiky bezpečnosti IT vymezím v této kapitole základní pojmy, které se ve spojení s bezpečností používají.

3.1.1 Informační systém

V širším kontextu používáme termín informační systém, který zahrnuje data, software, hardware, organizační prostředky, a v určité míře také lidské zdroje.

„Když analyzujeme IS z hlediska potřeb jeho zabezpečení, rozpoznáváme:

- Objekt IS – pasivní entita, která obsahuje/přijímá informace a je přístupná autorizovaným subjektům IS
- Subjekt IS – aktivní entita (osoba, proces nebo zařízení činné na základě příkazu uživatele) autorizovatelná pro získání informace z objektu, vydávání příkazů ovlivňujících udělení práv přístupu k objektu, změnu stavu objektu apod.“ (4, s.12)

3.1.2 Aktiva

Aktivum je prvek informačního systému, který organizace využívá nebo vlastní a má pro ni nezanedbatelnou hodnotu. Jedná se o myšlenky, postupy, data, software, hardware, atd.. Ztráta nebo snížení hodnoty aktiva organizaci způsobuje škodu a proto je třeba aktiva chránit. Zvláštním případem aktiv jsou citlivá aktiva, která mají významnou hodnotu z hlediska plnění cílů organizace. Škoda na citlivém aktivu ovlivňuje dosažitelnost těchto cílů a může ochromit chod společnosti.

3.1.3 Hrozba

Hrozbu představuje potenciální narušení bezpečnosti, které může mít za následek poškození systému nebo organizace a jejích aktiv. Fakt, že by k narušení mohlo dojít, vyžaduje této možnosti zabránit nebo na ni být alespoň připravený.

Hrozby mohou mít objektivní nebo subjektivní původ. Hrozba může vzniknout uvnitř organizace, např. zlomyslný zaměstnanec, nebo zvenku, např. útok hackera.

Hrozby dělíme na:

Tabulka 1: Dělení hrozeb

Druhy		Příklad
Objektivní (neovlivněny lidským faktorem)	Přírodní a fyzické	Požár, povodeň, výpadek napětí
	Fyzikální	Elektromagnetické záření, vlhkost
	Technické a logické	Porucha pevného disku, backdoor, špatné zapojení
Subjektivní (plynoucí z lidského faktoru)	Úmyslné	Krádež, hacking systému
	Neúmyslné	Chyby a opomenutí, fyzické nehody

3.1.4 Zranitelnost

Zranitelnost je skutečnost, která může být využita jednou nebo více hrozbami, a spočívá ve slabině některého bezpečnostního opatření nebo v jeho úplné absenci. Zranitelnost sama o sobě není příčinou škody, ale pouze podmínkou nebo množinou podmínek, které mohou umožnit hrozbě, aby ovlivnila aktiva.

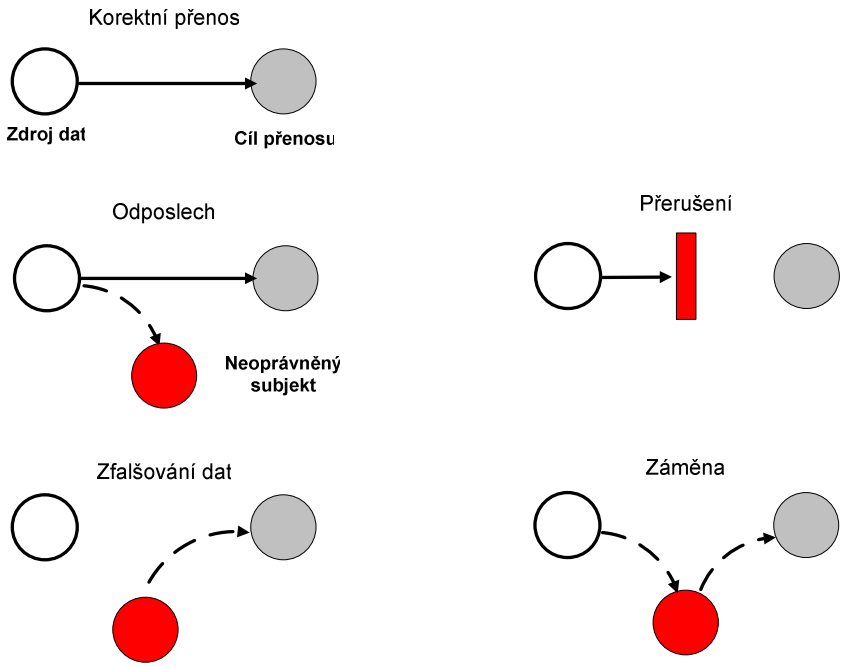
Mezi zranitelnosti se zahrnují funkční slabiny návrhu systému, provozování systému, případně slabiny bezpečnostních opatření navržených pro ochranu systému. Dále známe lokální slabiny, do kterých zahrnujeme slabiny ve fyzickém uspořádání, v organizaci, v postupech a procedurách, v personální politice, v managementu, v administraci systému, v hardware, v software, v informacích a informačních zdrojích, a podobně.

3.1.5 Útok a dopad

Útok je realizace hrozby a jeho důsledkem je škoda na aktivech, nebo-li dopad. Výraz útok je prakticky většinou používán pokud jeho původce je člověk, tedy útočník. Jako synonymum slova „útok“ se používá fráze „bezpečnostní incident“ a to pro útoky jak lidského tak i přírodního charakteru. Vážnost dopadu bezpečnostního incidentu můžeme rozdělit podle následující stupnice:

- Katastrofické – mají fatální následky v podobě zhroucení celé organizace nebo její trestní odpovědnost
- Významné – vážnou měrou poškozují organizaci
- Nevýznamné – způsobující zanedbatelné škody

Podle způsobu provedení útoku rozlišujeme následující typy útoků (grafické znázornění):



Obrázek 2: Typy útoků 10)

3.1.6 Útočník

Útočník je osoba s úmyslem zcizit, poškodit, či jinak znehodnotit aktiva organizace. Pokud chceme účinně zabránit útoku, je nutné nejdříve pochopit uvažování útočníka a jeho motivaci. Při návrhu ochrany je vhodné se dívat na celý problém jeho očima a uvědomit si možná rizika, která by nám jinak pravděpodobně unikla.

Podle pozice útočníka, ze které provádí útok, dělíme útočníky na:

- Externí – Tito útočníci na aktiva útočí z vně organizace. Snaží se získat přístup všemi možnými prostředky. Mají ztíženou situaci, protože například počítače s přímým přístupem na internet jsou z pohledu bezpečnosti konfigurovány přísněji. Musejí zdolávat překážky jako jsou hesla, firewally, atd.
- Interní – Většina útoků je vedena právě interními útočníky. Jedná se o útočníky napadající organizaci zevnitř. Jsou to převážně zaměstnanci s motivací se zaměstnavateli pomstít, získat informace pro konkurenci, uškodit dalším zaměstnancům, a další. Tito lidé většinou nebývají vzdělaní v oblasti informačních technologií tak jako útočníci externí. Na druhou stranu mají jistou výhodu, protože mají důvěru zaměstnavatele a fyzický přístup k síťovým prostředkům.

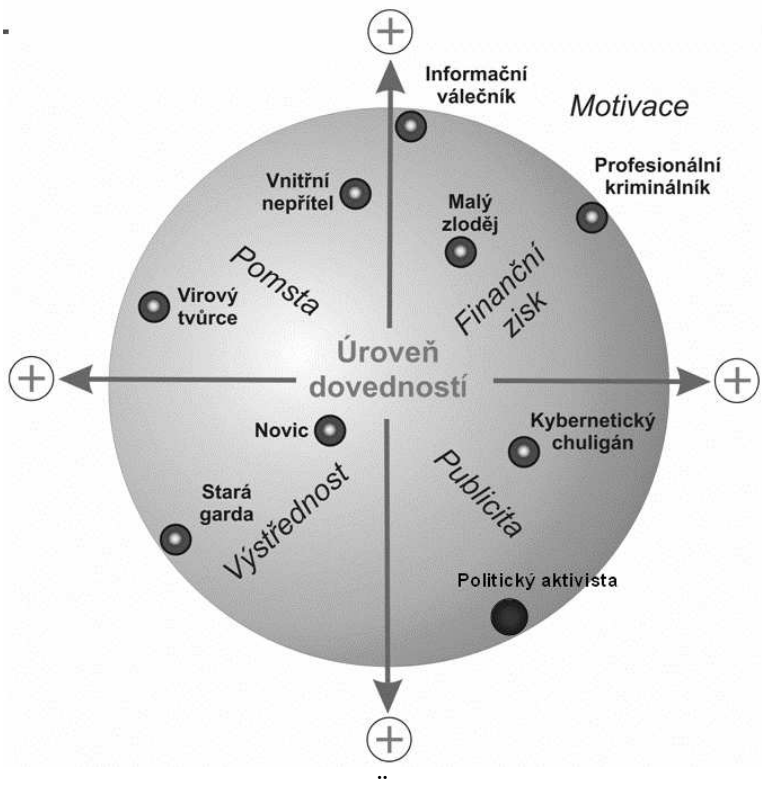
Podle odbornosti můžeme útočníky rozdělit na tři základní skupiny:

- Amatér – Tito útočníci disponují minimem znalostí z oblasti informačních technologií a o cíli jejich útoku. Využívají běžně dostupné předpřipravené nástroj a postupy pro útoky na známá zranitelná místa. Zkoušením pomocí těchto nástrojů metodou pokus-omyl nebo náhodným zjištěním zranitelnosti útočí na systémy. Pro zabezpečené systémy nepředstavují nebezpečí svými dovednostmi, ale svým velkým počtem. Jejich motivací může být například nalezení vzrušení.
- Hacker – Jsou to většinou inteligentní osoby nebo skupiny osob se schopnostmi programovat a základními znalostmi systému, na který chtějí útočit. Limitují je omezené finanční a výpočetní prostředky. Většinou nechtějí přímo nést vinu za útok, tak zpracovávají programové skripty, které

šíří v počítačové síti a provádí útok pomocí nich. Motivací může být zpřístupnění informací ostatním uživatelům, uznání hackerské komunity, nebo pomsta vedená proti konkrétní firmě, organizaci nebo zájmové skupině lidí.

- Profesionál – Jedná se o zkušené jedince nebo týmy s nákladným a sofistikovaným vybavením. Mají hluboké znalosti programování a nabourávání se do systémů. Mohou provádět detailní analýzy systému a navrhovat komplexní útoky. Jsou schopni se nabourat takřka do všech sítí a vyhnout se i detekci pokud mají dostatek času. Mohou být najímáni různými zločinnými organizacemi, vědomě porušovat zákony a jejich motivací může být finanční nebo jiný prospěch.

Existuje mnoho podrobnějších dělení útočníků. Následující obrázek kategorizuje útočníky podle kombinace dovedností a motivace.



Obrázek 3: Dělení útočníků 9)

3.1.7 Riziko

Riziko představuje vztah pravděpodobnosti využití zranitelnosti hrozbou (útočníkem) a dopadu uskutečnění hrozby (ztráta nebo poškození aktiv). Riziko popisujeme vztahem:

Riziko = pravděpodobnost hrozby * dopad uskutečnění hrozby

3.1.8 Bezpečnostní cíle

Bezpečnostní cíl je prvním krokem k prosazení bezpečnosti v podniku. V bezpečnostním cíli je zdokumentován stav, kterého má být v organizaci dosaženo. Nejsou v něm ještě uvedeny konkrétní požadavky na organizační, fyzickou, logickou a další bezpečnost.

Počítačová bezpečnost má základní trojici bezpečnostních cílů: důvěrnost, integrita a dostupnost (C-I-A; Confidentiality, Integrity, Availability). Tyto pojmy nyní rozvedu:

- Důvěrnost – Obecně je důvěrnost utajení informací nebo zdrojů. Soustředí se na omezení přístupu k informacím a prozrazení pouze oprávněným uživatelům, neboli „správným lidem“, a zamezení přístupu a prozrazení neoprávněným uživatelům, neboli „špatným lidem“. Důvěrnost úzce souvisí se soukromím osobních informací. Prakticky je cíle důvěrnosti dosahováno pomocí autentizačních metod, jako jsou například uživatelská jména a hesla, tokeny, biometrické identifikátory, apod.
- Integrita – Integrita se zabývá věrohodností informačních zdrojů. Definujeme pojem „datová integrita“, což znamená, že data nebyla nevhodně měněna, ať už v důsledku havárie či zlomyslnou činností. Další důležitý pojem je „původ“ neboli „zdrojová integrita“, tedy že data pochází od člověka nebo entity, od které si myslíme že pochází, než od podvodníka.
- Dostupnost – Dostupnost se zabývá zajištěním přístupu k informačním zdrojům v určitou dobu. Téměř všechny organizace jsou závislé na fungujících informačních systémech. Informační systém, který je nedostupný v momentu potřeby je stejně špatný jako systém žádný. Prakticky může být dostupnost ovlivněna technickými problémy (např.

chyba hardware), přírodními vlivy (např. povodeň) nebo lidskou chybou (úmyslnou nebo neúmyslnou).

3.1.9 Bezpečnostní funkce

Bezpečnostní funkce prosazují plnění bezpečnostních cílů a můžeme je rozdělit na:

- Preventivní - Prevence znamená, že hrozbu nebude možné uskutečnit. Pokud se bude například útočník snažit přes internet nabourat do počítače a tento počítač nebude k internetu připojený, předešli jsme útoku. Prevence tedy vyžaduje implementaci mechanismů, které není možné nijak obejít.
- Detekční – Detekci je vhodné uplatnit tehdy, pokud nejsme schopni útoku zabránit. Počítá s faktem, že k útoku může dojít a má za cíl detekovat jestli k útoku došlo nebo k němu právě dochází. Úkolem detekce je i monitorování akcí systému, které by naznačovali útok. Příkladem může být upozornění na vysoký počet nesprávně zadaných hesel.
- Opravné – Opravná funkce se nejprve pokusí o zastavení útoku a při úspěchu vyhodnotí škodu a pokusí se o její nápravu. Dále vyžaduje, aby bylo odstraněno zranitelné místo, přes které byl útok veden.

3.1.10 Bezpečnostní mechanismy

Bezpečnostní mechanismy jsou nástroje, pomocí nichž implementujeme bezpečnostní funkce.

Bezpečnostní mechanismy kategorizujeme podle jejich povahy na:

- Fyzické – zámky, trezory, protipožární ochrana, stínění, atd.
- Technické – ID karty, autentizační kalkulátory, atd.
- Logické – digitální podpisy, kryptografie, kódování, atd.
- Administrativní – hesla, předpisy, přijímací a výpovědní postupy, atd.

3.2 Bezpečnostní politika

Tato bakalářská práce se zabývá „bezpečnostní politikou“ a proto v této kapitole objasním co to vlastně je a co obsahuje.

Když mluvíme o bezpečnostní politice tak si musíme ujasnit jaký typ bezpečnostní politiky máme na mysli. Bezpečnostní politiky bývají uspořádány hierarchicky.

„Celková bezpečnostní politika je zaměřena na kompletní aktiva organizace, zabývá se nejen informačním systémem a daty v něm zpracovávanými, ale také zásobami, investičním majetkem či bezpečností práce. Celková bezpečnostní politika úzce souvisí s dlouhodobými strategickými záměry organizace. Součástí celkové bezpečnostní politiky je systémová bezpečnostní politika. Systémová bezpečnostní politika má za úkol zajistit aktiva, která jsou součástí informačního systému. Data bývají často jedním z nejcennějších aktiv, je třeba jim proto věnovat velkou pozornost.“ 15)

V této práci se tedy, podle definice, zabývám systémovou bezpečnostní politikou, kterou označuji jako „bezpečnostní politika“.

3.2.1 Co je to bezpečnostní politika

Bezpečnostní politika je dokument definující základní principy vedoucí k prosazení bezpečnostních funkcí organizace s dlouhodobou platností a je víceméně nezávislý na aktuálních informačních technologiích používaných v organizaci. Cíl bezpečnostní politiky je poskytnout směr a podporu pro informační bezpečnost v souladu s požadavky organizace a příslušnými právními normami.

Bezpečnostní politika může mimo jiné odpovídat na následující otázky:

- Co chceme chránit?
- Jak to chceme chránit?
- Jak to budeme kontrolovat, zda je to chráněno?
- Kdo za to nese odpovědnost a jaké budou sankce při porušení?

Na tyto základní otázky nám pomáhá odpovědět identifikace a ohodnocení aktiv, tedy především dat, které máme v organizaci.

3.2.2 Náležitosti bezpečnostní politiky

Existují různé názory na to, co má bezpečnostní politika přesně obsahovat. Faktem je, že každá organizace se bezpečnostní politikou zabývá s různou mírou pečlivosti.

Obsáhlejší bezpečnostní politika může vypadat například takto:

Tabulka 2: Náležitosti bezpečnostní politiky

Bezpečnostní politika organizace X	
Přehled	Důvody proč politika existuje. Co v ní je zahrnuto a co v ní zahrnuto není.
Rozsah platnosti	Rozsah platnosti určuje koho se tato politika týká a jakého informačního vybavení se týká.
Role a odpovědnosti	Kdo má jaké role a odpovědnosti pod touto bezpečnostní politikou.
Sankce při nedodržení	Jakmile jsou vysvětleny role a odpovědnosti, je potřeba uvést jaké sankce těmto osobám hrozí při nedodržení pravidel bezpečnostní politiky.
Analýza rizik	Identifikace(klasifikace) aktiv a jejich ceny, jaké hrozby jim hrozí, apod.
Bezpečnostní opatření	Tato část je nejobsáhlejší. Zavádí pravidla, která říkají jaká aktiva je třeba chránit a jakým způsobem toho dosáhneme. Tyto pravidla musejí být přehodnoceny vždy, když dojde ke změně aktiv.
Odkazy na související dokumenty	Odkázání na dokumentaci podporující bezpečnostní politiku. Mohou to být doplňující směrnice, havarijní plány a podobně.
Revize	Určuje například pravidla a intervaly provádění revize bezpečnostní politiky.

3.2.3 Revize

Bezpečnostní politika je považovaná za „živý“ dokument. To znamená, že vzhledem k neustále se měnícím podmínkám organizačního prostředí, právních podmínek či technickému prostředí je zapotřebí bezpečnostní politiku neustále upravovat. Je dobré provádět revizi bezpečnostní politiky v plánovaných intervalech nebo při vzniku nečekaných změn. Revize by měla obsahovat návrhy na vylepšení bezpečnostní politiky a řízení informační bezpečnosti.

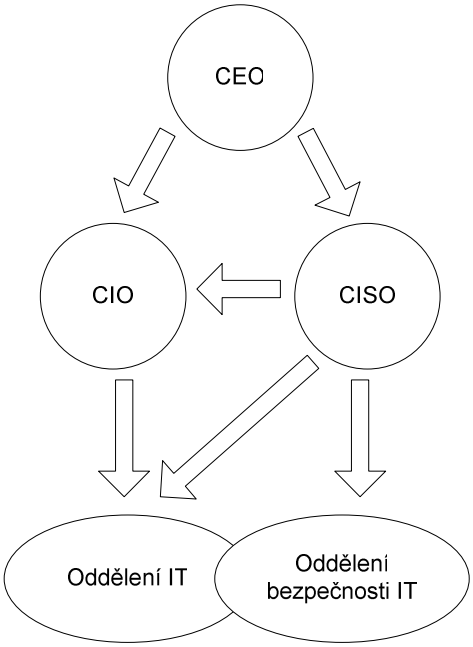
3.3 Personální zajištění bezpečnosti

Jednou z hlavních otázek, kterou se zabýváme při tvorbě řízení bezpečnosti je její personální zajištění. Musíme určit kdo bude mít bezpečnost na starosti, kdo za ni bude zodpovědný a kdo o ní bude rozhodovat.

Může nás napadnout zařadit oblast bezpečnosti pod IT oddělení. Sice to budou v konečném důsledku právě pracovníci IT oddělení, kteří se budou starat o zabezpečení počítačů, ale my potřebujeme někoho, kdo bude řídit zavádění bezpečnosti. Pak nás tedy napadá ředitel IT oddělení, neboli CIO (Chief Information Officer). V menších firmách by se problém takto dal vyřešit. V malých firmách, kde není ani CIO, je možné problém vyřešit outsourcingem odborné firmě. Ve větších firmách by měl za bezpečnost zodpovídat někdo jiný než CIO a to z důvodu částečné protichůdnosti požadavků na IT oddělení a oddělení bezpečnosti.

Vytvoříme funkci ředitele bezpečnosti, který je přímo podřízen generálnímu řediteli (CEO), a nazveme ho CISO (Chief Information Security Officer). „S ředitelem IT je služebně na stejné úrovni, měl by být ale vybaven potřebnými pravomocemi pro případ krizových situací. Jen u opravdu velkých firem existuje zvláštní oddělení bezpečnosti IT, většinou je tedy CISO nadřízen oddělení IT.“ (2, s.167)

„Hlavním posláním ředitele bezpečnosti je analyzovat současný stav a navrhnout jeho zlepšení. Za tímto účelem vytváří bezpečnostní politiku dané firmy a prostřednictvím svých pravomocí zajišťuje její zavedení do běžné vnitrofiremní praxe. Podle měnících se požadavků zaměstnanců a vedení firmy zajišťuje průběžnou aktualizaci bezpečnostní politiky.“ (2, s. 167)



Obrázek 4: Firemní hierarchie pro řízení bezpečnosti (2, s. 166)

3.4 Analýza rizik

Analýza rizik je jedním z nejdůležitějších kroků při tvorbě bezpečnostní politiky. Nevhodně provedená analýza rizik má takřka vždy za následek chybně zvolená bezpečnostní opatření. Aktiva pak mohou být chráněna velmi nákladným, ale ne zcela účinným způsobem.

„Analýza rizik se skládá z několika kroků:

- Identifikace aktiv
- Identifikace hrozeb
- Vlastní analýza rizik“ (doseděl 170)

3.4.1 Identifikace aktiv

Ve fázi identifikace aktiv je velmi důležité porozumět informačnímu systému a jak funguje. Úkolem je zjistit jaká aktiva se v systému vyskytují a určit jejich hodnotu pro společnost. Je doporučeno spolupracovat s oddělením IT, jelikož jeho pracovníci nejlépe vědí, jaká data se ve firmě zpracovávají a ukládají.

Vytvoříme seznam ukládaných dat, nejlépe v obecné řeči, která vystihuje povahu dat. Toto opatření provádíme proto, aby běžní uživatelé mohli lépe určit cenu těchto dat,

protože to budou právě oni, koho se budeme dotazovat. Hodnotu dat budou stanovovat „vlastníci“ těchto dat. Je zřejmé, že pro každého budou mít konkrétní data odlišnou hodnotu a proto musíme brát v úvahu vždy tu nejvyšší.

3.4.2 Identifikace hrozeb

O něco složitější než identifikace aktiv je identifikace hrozeb, které aktivům hrozí. Seznam hrozeb je v čase proměnlivý, proto se zde vyskytuje nebezpečí, že na něco zapomeneme. K identifikaci hrozeb můžeme přistupovat následujícími způsoby:

- Přemýšlíme nad všemi situacemi, které mohou v systému nastat. Zkoumáme různé otázky (např.: Co když vyhoří serverovna?). Je velmi pravděpodobné, že nás nenapadnou všechny scénáře. Proto je dobré nad problémem neustále přemýšlet a seznam hrozeb aktualizovat.
- Obstaráme si již vytvořený seznam hrozeb z podobného prostředí. Můžeme jej získat například od firmy zabývající se bezpečností. V tomto případě nesmíme ovšem zapomenout tento seznam přizpůsobit našim podmínkám anebo se ho pokusit doplnit o možné hrozby, na které bylo zapomenuto.
- Využijeme podrobný dotazník přizpůsobený pro naše prostředí. Tento dotazník vyplňuje bezpečnostní expert a bod po bodu zjišťuje možné hrozby. Pokud je dotazník pečlivě navržen, tak je minimalizováno riziko, že bude na něco zapomenuto.

3.4.3 Vlastní analýza rizik

Po provedení identifikace aktiv a identifikace hrozeb máme dva seznamy – seznam aktiv a jejich ohodnocení, a seznam hrozeb, které aktivům hrozí. Vlastní analýza rizik má za úkol zjistit jaká nebezpečí hrozí jakým aktivům.

Při procházení seznamu aktiv rozhodujeme, které hrozby se k jednotlivým aktivům vztahují. Konkrétní hrozba se může vztahovat k více aktivům a ke konkrétnímu aktivu se může vztahovat více hrozeb. Výsledkem je seznam aktiv a jim přiřazených hrozeb. Každé kombinaci aktivum-hrozba přiřazujeme pravděpodobnost, s jakou dojde ke hrozbě u daného aktiva. Můžeme pak stanovit hranici pravděpodobnosti hrozeb, proti kterým se budeme chránit. Protože se aktiva, jejich hodnota i hrozby mění, je nutné provádět analýzu opakovaně v určitých časových intervalech.

3.4.4 Navržení vhodné ochrany

Jakmile máme stanovené pravděpodobnosti hrozeb a hranici pravděpodobnosti hrozeb, proti kterým se chceme chránit, budeme navrhovat jednotlivé ochrany. Krok navržení vhodné ochrany se sice nezahrnuje do analýzy rizik, ale bezprostředně po ní následuje.

„Ochrana by měla být navržena pro každou dvojici aktivum-hrozba, často ale dojde k situaci, kdy jeden použitý bezpečnostní prostředek zajistí ochranu více takových dvojic. Jako ideální způsob návrhu se tedy jeví postup shora dolů. U každé dvojice navrhneme odpovídající ochranu a vyčíslíme náklady na její zavedení a udržování“. (2, s. 172).

Posledním krokem je prosadit jednotlivé ochrany. Řídíme se pravidlem: Ochranu aplikujeme tehdy, když náklady na její zavedení nepřevyšují hodnotu chráněných aktiv.

3.5 Havarijní plány

Jako havárii nebo krizový stav systému označujeme stav, kdy dojde k selhání bezpečnostních opatření. Po havárii je nutné co nejdříve obnovit důležité části informačního systému a poškozená data.

Obnova se provádí podle následujících kroků:

- Odstranění akutního nebezpečí: podle druhu katastrofy, která nás postihla.
- Obnovení důležitých částí systému: výměna poškozeného hardware, reinstalace software, atd.
- Obnovení poškozených dat: obnova dat z poslední nepoškozené záložní kopie
- Zavedení příslušných opatření: po havárii se poučíme z chyb a snažíme se těmto případům předejít v budoucnu. Můžeme například vydat nové směrnice, které se snaží uskutečněné havárii zabránit.

Pro případy havárií vypracováváme havarijní plány, které jasně stanovují kroky a jejich pořadí při řešení havarijních situací. Je důležité určit, kdo a jak určuje nastání krizového stavu, a kdo a jak určuje ukončení tohoto stavu.

Havarijní plán by se měl zabývat těmito záležitostmi:

- Vyhlášení a zrušení havarijního stavu – Objasňuje co to havarijní stav je, kdo a jak ho vyhlašuje, podmínky jeho vyhlášení, kdy stav pomíjí a kdo ho může rušit.
- Personální zajištění – Stanovuje pravomoci řízení při havarijním stavu. Při tvorbě této části je vhodné spolupracovat s personálním oddělením. Dále je zde stanoveno jak bude informováno vedení a zaměstnanci o vyhlášení, průběhu a řešení havarijního stavu.
- Postup pro konkrétní havarijní stavy – Určuje konkrétní postupy pro řešení jednotlivých typů havárií.
- Administrativní záležitosti – Obsahuje informace o havarijním plánu jako dokumentu. Stanovuje kdo a jak bude vyškolen, kde bude dokument uložen, jak se bude kontrolovat a aktualizovat, atd.

Havarijní plán by měl být uložen odděleně od bezpečnostní politiky alespoň v jedné kopii v bezpečném a dostupném prostředí.

3.6 Zálohování

Zálohování je proces vytváření kopií dat nebo operačního systému tak, že tyto kopie můžeme použít pro obnovu původních dat po havárii nebo ztrátě těchto dat. Tyto kopie nazýváme zálohy. Pojem zálohování je často zaměňován s pojmem archivace. Archivy jsou kopie, které se odkládají pro případné další užití, narozdíl od záloh, které mají být dostupné, když bude potřeba obnovit původní data.

Zálohování má tedy za cíl co nejdříve obnovit poškozená, smazaná, či jinak znehodnocená data. Ke zničení dat může dojít v zásadě dvěma způsoby. Buď jsou data smazána nebo poškozena na svém nosiči nebo je zničen jejich nosič. Při obnově ze záloh ovšem o určitá data vždy přicházíme a to ta, která byla vytvořena od posledního zálohování. V současné době existuje velké množství sofistikovaných zálohovacích

zařízení a programů, které umožňují nastavit různé pokročilé funkce, aby proces zálohování byl co nejpohodlnější.

Při řešení problematiky zálohování je nutné odpovědět na otázky:

- Co se bude zálohovat – Protože zálohování není levná záležitost a v organizacích se vyskytují různě důležitá data, je třeba určit jaká data mají při zálohování prioritu. Určitě bude nutné zálohovat databáze zákazníků nebo účetní data, která mají pro firmu hodnotu, oproti například instalačním souborům freeware staženého z internetu.
- Frekvence zálohování – Jak často zálohujeme závisí na tom, jak často se data mění v kombinaci s tím, jak jsou změny v nich důležité. V organizacích, kde se pracuje každý den, se doporučuje zálohovat denně a tak můžeme přijít o maximálně jeden den práce.
- Na co se bude zálohovat – Nejdůležitější je volba média, na které zálohujeme. Nejoblíbenější řešení pro objemné zálohy je magnetická páska, kvůli své ceně a možnosti přenášení tohoto média. Větší popularitu ovšem získává zálohování na pevné disky, protože jejich cena klesá. Potenciál má také zálohování přes síť nebo internet do vzdálené lokality například na disková pole.

Typy záloh jsou:

- Úplná – Při této metodě zálohování se zálohují vždy všechny soubory určené k záloze. Výhodou je rychlá obnova a záporem dlouhá doba zálohování, protože kopírujeme všechna data. K obnovení ze zálohy je potřeba jen poslední úplná kopie.
- Rozdílová – Při první úplné záloze se soubory označí jako zálohované. Při rozdílové záloze se pak zálohují jen ta data, která byla od poslední úplné zálohy změněna. Při další rozdílové záloze se opět zálohují všechna data změněné od poslední úplné zálohy, a tedy i ta vytvořená při předchozí rozdílové. Pokud chceme data obnovit, je třeba obnovit poslední úplnou zálohu a následně poslední rozdílovou zálohu.

- Přírůstková – Zálohují se pouze soubory vytvořené nebo změněné od posledního úplného nebo přírůstkového zálohování. Po záloze je soubor označen jako zálohovaný a při jeho změně je označení odebráno. Při kombinaci úplného a přírůstkového zálohování je pro obnovu dat nutné mít poslední úplnou zálohu a všechny přírůstkové zálohy.

Vytvořené zálohy je v prvé řadě nutné skladovat v jiném místě než jsou původní data. To je důležité opatření proti přírodním katastrofám nebo krádeži. Neméně důležité opatření je pravidelná kontrola záloh, aby jsme si byli jisti, že v případě potřeby bude obnova dat úspěšná.

3.7 Normy a zákony

V České republice je používání bezpečnostních norem, oproti zákonům, pouze doporučené. Tyto normy jsou vydávány nadnárodními organizacemi. Vybrané normy překládá z angličtiny a vydává Český normalizační institut. Při řešení bezpečnosti se řídíme:

- Normy ISO – jsou vydávány International Organization for Standardization
- Normy IEC – jsou vydávány International Electrotechnical Commission
- Normy ITU – jsou vydávány International Telecommunications Union
- Legislativa ČR

3.7.1 Norma ISO/IEC 13335

Jako jedna z ústředních norem řízení bezpečnosti se považuje ISO/IEC 13335 s názvem Informační technologie – Soubor postupů pro management bezpečnosti informací. Je určená převážně manažerům zodpovědným za bezpečnost IT.

Česká verze má tyto části:

- ČSN ISO/IEC TR 13335-1 - Pojetí a modely bezpečnosti IT
- ČSN ISO/IEC TR 13335-2 - Řízení a plánování bezpečnosti IT
- ČSN ISO/IEC TR 13335-3 - Techniky pro řízení bezpečnosti IT
- ČSN ISO/IEC TR 13335-4 -Výběr ochranných opatření

3.7.2 Norma ISO/IEC 17779:2005

Norma ISO/IEC 17779:2005 je velmi obsáhlá a zaměřuje se na pravidla a principy pro vytvoření bezpečnostní politiky. Bezpečnostní kontroly, prostředky řízení rizika, uváděné v této normě by neměly být všechny použity. Vhodné kontroly se vybírají pro specifické potřeby organizace po důkladné analýze rizik. Oblasti pokryté touto normou jsou:

- Bezpečnostní politika – Definuje co to bezpečnostní politika je, co má obsahovat a jak se má aktualizovat
- Organizace bezpečnosti – Popisuje organizační opatření pro řízení bezpečnosti ve firmě.
- Řízení aktiv – Doporučuje udržovat přiměřenou ochranu aktiv, aby měla svého vlastníka a ten za ně nesl odpovědnost. Dále mluví například o klasifikaci aktiv, aby jim mohla být poskytnuta přiměřená ochrana.
- Bezpečnost lidských zdrojů – Věnuje se například prověřování zaměstnanců před nástupem do povolání, jejich školení v průběhu zaměstnání nebo snížení rizika zneužití prostředků organizace.
- Fyzická bezpečnost a bezpečnost prostředí – Popisuje opatření jak předcházet neautorizovanému přístupu do vymezených prostor a poškození a zásahům do provozních budov a informací organizace.
- Řízení komunikací a řízení provozu - Cílem je zajistit správný a bezpečný provoz prostředků pro zpracování informací. Měly by být stanoveny odpovědnosti a postupy pro řízení a správu prostředků zpracovávajících informace.
- Řízení přístupu – Poskytuje doporučení jak předcházet neoprávněnému přístupu k informačním systémům, jak postupovat při přidělování uživatelských práv, odpovědnosti uživatelů, atd.
- Vývoj a údržba systémů - Cílem je zajistit implementaci bezpečnosti do informačních systémů. To zahrnuje infrastrukturu, organizaci a uživatelsky vyvinuté aplikace.

- Řízení kontinuity činností organizace - Cílem je bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných chyb a katastrof.
- Soulad s požadavky – Zdůrazňuje jak je nutné se vyvarovat porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

3.7.3 Norma ISO/IEC 27001:2005

V roce 2005 vydala ISO normu 27001:2005 s názvem Požadavky na systém řízení bezpečnosti informací. Tato norma vychází ze zmíněné ISO/IEC 13335.

„Norma ISO/IEC 27001 si klade za cíl poskytnout doporučení, jak aplikovat ISO/IEC 17799 (do budoucna ISO/IEC 27002) v rámci procesu ustavení, provozu, údržby a zlepšování systému řízení bezpečnosti informací (ISMS) v organizaci v souladu se systémy řízení kvality nebo bezpečnosti prostředí. Norma popisuje vhodný systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO/IEC 17799.“ 18)

„Mezi hlavní aspekty této normy patří:

- harmonizace s normami pro další systémy řízení
- kontinuální zajištění procesu zlepšování řízení bezpečnosti informací
- celopodnikové řízení
- zajištění souladu s právními a regulatorními předpisy
- záruky za bezpečnost informací
- zavedení principů OECD pro bezpečnost informačních systémů a sítí“ 18)

3.7.4 Legislativa ČR

V poslední době velmi sledovaný zákon v souvislosti s informační bezpečností je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

„Účelem zákona je zajistit ochranu osobních údajů, způsob jejich zpracování v České republice a předávání osobních údajů do zahraničí, a upravit vztahy, které v souvislosti s nimi vznikají.“ 8)

„Za osobní údaje se považují takové údaje, které se vztahují k fyzické osobě, na jejichž základě je konkrétní fyzická osoba určena nebo určena být může. Přitom platí, že taková osoba je určena či určitelná, pokud pomocí jednoho či více osobních údajů lze určit její identitu. Může jít o jeden údaj, např. fotografie, ale zpravidla půjde o jejich soubor. Osobním údajem nemusí být bez dalšího jméno a příjmení a to dokonce ani ve spojení s adresou, protože v tomtéž místě může žít i více osob stejného jména a příjmení. Osobním údajem je vždy spojení jména, příjmení a rodného čísla, protože na jejich základě lze vždy fyzickou osobu identifikovat. Subjektem osobních údajů může být výlučně fyzická osoba, a to i cizinec, subjektem údajů však zásadně nemůže být právnická osoba.“ 8)

4 Návrh řešení

Analytická část práce odhalila několik různě vážných nedostatků v současné bezpečnostní politice firmy. Hlavním cílem firmy v oblasti bezpečnosti je ochránit svá data, protože představují nejcennější aktiva firmy. Vzhledem k omezenému rozsahu této práce se budu věnovat návrhu řešení bezpečnostní politiky z pohledu organizačního zajištění bezpečnosti dat. V této části se prakticky stavím do pozice ředitele bezpečnosti, který stanovuje bezpečnostní cíl a strategii firmy a určuje role, odpovědnosti a pravomoci, čímž pokládá základ pro vytvoření a provádění bezpečnostní politiky firmy.

Navrhuji:

- upravit a doplnit bezpečnostní cíle a strategii firmy
- vytvořit organizační strukturu bezpečnosti z pohledu zajištění bezpečnosti dat
- přidělit jednotlivým funkcím náležité odpovědnosti a pravomoci
- vytvořit příslušné směrnice a předpisy

4.1 Bezpečnostní cíl a strategie firmy

Současným cílem firmy v oblasti bezpečnosti je zaručit svým datům 100% ochranu, protože představují nejcennější část aktiv firmy. V běžné praxi je uskutečnění tohoto požadavku naprosto nereálné. Strategii firmy představuje opatření chránit data proti vnějším útočníkům a škodlivému kódu. V tomto případě ovšem firma nemá kompletně stanovenou bezpečnostní strategii jak cíle dosáhnout a cíl je příliš stručný.

Navrhuji upravit bezpečnostní cíl firmy: Cílem ohledně bezpečnosti informací ve firmě je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření.

V případě menších firem, na rozdíl od velkých korporací, odpadá potřeba vytvářet obsáhlou bezpečnostní strategii.

Navrhuji upravit bezpečnostní strategii firmy:

1. Funkci pro řízení bezpečnosti vykonává ředitel bezpečnosti (CISO).
2. Provádění bezpečnostní politiky zajišťují vedoucí pracovníci podle jejich působnosti a odpovědnosti.
3. Data jsou chráněna pomocí pravidel pro jejich klasifikaci a řízení.
4. Je zajištěno, aby k datům měli přístup jen oprávněné osoby.
5. Data jsou zálohována a to tak, aby v případě havárie bylo možno data co nejdříve obnovit.
6. Jsou zavedeny vhodné postupy pro přijímací řízení, ukončení pracovního poměru zaměstnanců a jejich vzdělávání o bezpečnosti během jejich zaměstnání.
7. Je stanoveno zajištění fyzické ochrany a ochrany prostředí, ve kterém se data nacházejí.

Od této strategie se odvíjí vytvoření organizační struktury bezpečnosti IS/IT, odpovědností a směrnic.

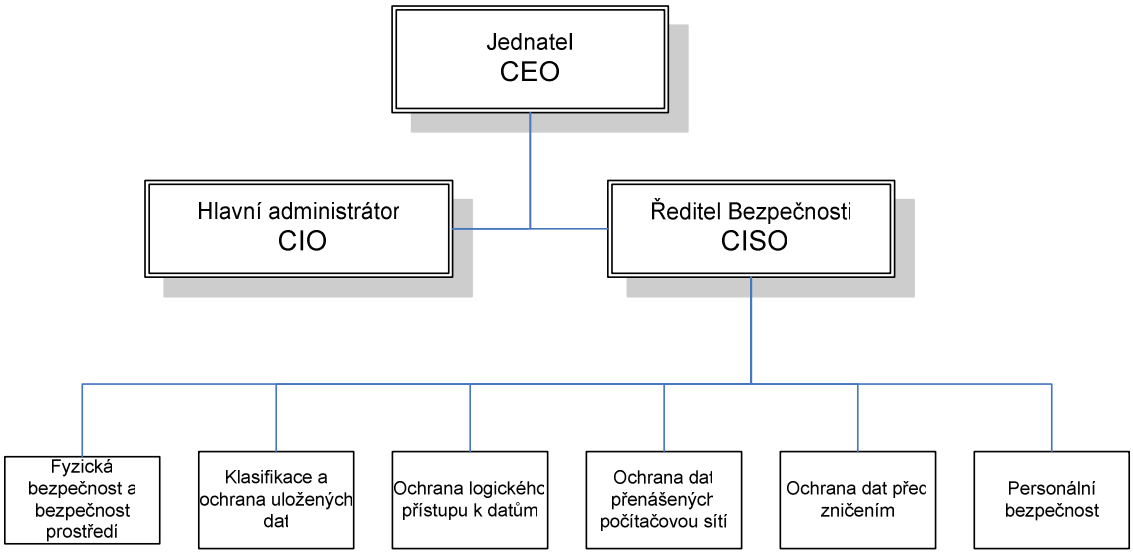
4.2 Organizační struktura bezpečnosti IS/IT

V současné době ve firmě figuruje pouze hlavní administrátor z firmy externího správce IT jako CIO, který se má starat také o zabezpečení. Prakticky ale otázky bezpečnosti řeší velice okrajově. Toto opatření považuji za nedostačující a proto navrhuji vytvořit několik nových funkcí pro bezpečnost.

Navrhuji vytvořit funkci ředitele bezpečnosti CISO, který se zodpovídá jednateli za zajištění bezpečnosti ve firmě. Pod ředitelem bezpečnosti navrhuji vytvořit funkce pro fyzickou bezpečnost a bezpečnost prostředí, klasifikaci a ochranu uložených dat, ochranu logického přístupu k datům, ochranu dat přenášených počítačovou sítí, ochranu dat před zničením a personální bezpečnost. Zmíněná funkční místa znázorňují dílčí oblasti zajištění bezpečnosti ve firmě (viz. obrázek 5). Pracovníci, kteří je mají v popisu

práce, zodpovídají řediteli bezpečnosti za korektní navrhnutí směrnic. Ředitel bezpečnosti kontroluje stav dodržování směrnic, navrhuje jejich úpravy a deleguje pravomoci pro jejich vykonávání.

Je nutné zdůraznit, že konkrétnímu pracovníkovi můžeme přiřadit jednu nebo více funkcí bezpečnosti. Vycházím z proměnlivé a různé časové náročnosti navržených funkcí.



Obrázek 5: Návrh organizační struktury bezpečnosti IS/IT

Při návrhu na vytvoření jednotlivých směrnic určuji kdo je vytvoří, popis jejich obsahu, kdo kontroluje jejich dodržování a sankce při nedodržení. Všechny směrnice vytvářejí pracovníci externího správce IT (popřípadě jiné firmy zabývající se bezpečností), kteří jsou pro dané oblasti nejlépe kvalifikovaní. Pokud je to potřeba, tak spolupracují na návrhu s příslušným zaměstnancem firmy. Navrhované směrnice jsou závazné pro všechny zaměstnance. Dodržování směrnic je kontrolováno vybranou osobou. Aby se zamezilo jejich porušování, navrhuji stanovit finanční sankce. Tyto sankce navrhuji realizovat jako srážky z pohyblivé složky mzdy zaměstnance. Pravidla pro udělování sankcí a jejich výši stanoví hlavní personalista ve směrnici o sankcích, na jejíž tvorbě se bude podílet.

4.3 Fyzická bezpečnost a bezpečnost prostředí

Pracovník, který má v popisu práce funkci fyzického zabezpečení, zodpovídá za zabezpečení fyzického přístupu k datům a aby data byla uchovávána v co nejlepších fyzikálních podmínkách. Jsou mu poskytnuty plány budov, požární plány, přístup k prvkům kamerového systému a přístup do prostor obsahující důležitá data firmy. Mapuje pohyb osob po prostorách se servery a kritickými daty.

Navrhuji vytvořit následující směrnice:

- **Směrnice o fyzickém přístupu a pohybu osob ve firemních prostorách**

  Vytvoří: Pracovník zajišťující fyzickou bezpečnost a bezpečnost prostředí ve spolupráci s firemním personalistou a správcem dané lokality

  Popis: Je zde popsáno, co musí vykonat zaměstnanec při příchodu a odchodu z práce (povinnost převzít a odevzdat klíče od kanceláře, označit příchod/odchod čipovou kartou), kam mají zaměstnanci přístup a kam ne, co dělat při ztrátě klíčů nebo čipové karty. Je zde popsána úloha recepce, jak se evidují návštěvy, jak se přijímají, povinnost doprovodu, atd.

  Kontroluje: Hlavní personalista

  Sankce: Za nedodržení navrhuji udělit zaměstnanci sankci až do výše 5000 Kč z pohyblivé složky mzdy.

- **Směrnice o fyzické bezpečnosti serverových místností**

  Vytvoří: Pracovník zajišťující fyzickou bezpečnost a bezpečnost prostředí
  Popis: Určuje jakým způsobem se bude evidovat pohyb osob po serverových místnostech, kdo do nich bude mít přístup a způsob práce v těchto místnostech. Jsou zde popsána protipožární opatření, klimatické podmínky, pravidla pro práci s UPS, požadavky na dveře a umístění počítačového vybavení.

  Kontroluje: Ředitel bezpečnosti IT

  Sankce: Za porušení navrhuji udělit zaměstnanci sankci až do výše 10000 Kč z pohyblivé složky mzdy.

- **Směrnice o fyzické bezpečnosti klientských stanic**

  Vytvoří: Pracovník zajišťující fyzickou bezpečnost a bezpečnost prostředí
  Popis: Stanovuje pravidla pro fyzické uložení přístrojů tak, aby se nepřehřívaly, nenasávaly prach, aby bylo zamezeno jejich krádeži nebo neoprávněnému přemísťování a užívání, atd. Určuje jakým způsobem bude vedena jejich evidence a za jakých okolností je bude možné přemísťovat v rámci firmy i mimo ni. Dále stanovuje zákazy neoprávněných zásahů do konfigurace a jaká externí hardwarová zařízení lze či nelze připojovat.

  Kontroluje: Administrátor v rámci běžné správy

  Sankce: Za porušení navrhuji udělit zaměstnanci sankci až do výše 3000 Kč z pohyblivé složky mzdy.

- **Směrnice o fyzické bezpečnosti notebooků a přenosných zařízení**

  Vytvoří: Pracovník zajišťující fyzickou bezpečnost a bezpečnost prostředí
  Popis: Určuje jakým způsobem bude vedena jejich evidence a která zařízení bude nutné chránit a jakým způsobem. Stanovuje pravidla pro fyzické uložení přístrojů, aby bylo zamezeno jejich krádeži nebo neoprávněnému užívání. Dále stanovuje zákazy neoprávněných zásahů do konfigurace a jaká externí hardwarová zařízení lze či nelze připojovat.

  Kontroluje: Ředitel bezpečnosti IT

  Sankce: Za porušení navrhuji udělit zaměstnanci sankci až do výše 3000 Kč z pohyblivé složky mzdy.

4.4 Klasifikace a ochrana uložených dat

Pří analýze firemních dat jsem zjistil, že ve firmě neexistuje směrnice, která by se věnovala třídění dat podle jejich citlivosti a hodnoty pro firmu. V důsledku toho zaměstnanci nerozlišují, jak se k různým typům dat chovat a prakticky se všemi daty zacházejí stejně, což považuji za nevyhovující stav.

Pracovník, který má v popisu práce funkci klasifikace a ochrany uložených dat, nejprve vytváří předpis, ve kterém stanoví klasifikační úrovně a podle nich budou data roztříděna v závislosti na jejich citlivosti a hodnoty pro firmu. Pracovník řeší také problém jak budou uložená data zabezpečena. Je mu umožněn přístup k reprezentativnímu vzorku firemních dat a je seznámen s tím, kam se data a jejich kopie ukládají, kdo je vytváří, kdo s nimi pracuje a jak obíhají ve firmě.

Navrhuji vytvořit následující směrnice:

- **Směrnice o klasifikaci firemních dat**

  Vytvoří: Pracovník zajišťující klasifikaci a ochranu uložených dat ve spolupráci s vedoucími oddělení, kterých se data týkají

  Popis: Tento předpis vytváří klasifikační stupnici, přiřazuje klasifikační úrovně datům podle jejich hodnoty/citlivosti (viz. příloha 1) a určuje vlastníky dat, kteří jsou za ně zodpovědní.

  Kontroluje: Vedoucí oddělení, jež data vlastní, kontroluje správné třídění dat podle klasifikačních úrovní.

  Sankce: Sankce nejsou, jedná se o předpis

- **Směrnice o ochraně uložených dat a dat uložených na přenosných médiích**

  Vytvoří: Pracovník zajišťující klasifikaci a ochranu uložených dat

  Popis: Směrnice popisuje jak budou data chráněna proti škodlivému kódu a stanovuje, která ukládaná data (klasifikační úrovně) se budou šifrovat, jakými metodami to bude prováděno a jak je třeba zacházet s šifrovacími klíči. Dále podle klasifikačních úrovní upravuje kdo a jak k datům smí přistupovat, jak budou označena a jak se budou likvidovat až nebudou potřeba. Směrnice upřesňuje na jaká přenosná média se ve firmě data smí ukládat, na jaká se ukládat nesmí a jak manipulovat s přenosnými médii obsahující citlivá data.

  Kontroluje: Ředitel bezpečnosti IT a vedoucí oddělení, jež data vlastní

Sankce: Při nedodržení navrhuji udělit zaměstnanci sankci až do výše 10000 Kč z pohyblivé složky mzdy.

4.5 Ochrana logického přístupu k datům

Pracovníka, který má v popisu práce funkci pro ochranu logického přístupu k datům, je nutné seznámit s autentizačními metodami používanými ve firmě a s požadavky vlastníků dat na jejich logické zabezpečení.

Navrhuji vytvořit následující směrnice:

- **Směrnice o identifikaci a autentizaci uživatelů**

  Vytvoří: Pracovník zajišťující ochranu logického přístupu

  Popis: Směrnice stanovuje kritéria pro: uživatelská jména, tvorbu silných hesel (délka, povinné znaky, zakázaná slova), bezpečnou manipulaci s hesly, minimální stáří, maximální stáří a hloubku historie hesel. Je zde určeno kdo vytváří uživatelské účty a kdo je ruší. Je zde popsána práce s čipovými kartami a tokeny pro dvoufaktorovou autentizaci.

  Kontroluje: Ředitel bezpečnosti IT, většina pravidel je automaticky vynucena systémem

  Sankce: Za porušení navrhuji srazit zaměstnanci až 10000 Kč z pohyblivé složky mzdy.

- **Směrnice o řízení přístupu**

  Vytvoří: Pracovník zajišťující ochranu logického přístupu

  Popis: Tato směrnice určuje kdo a na základě jakých podmínek (např.: klasifikační úrovně dat) uděluje patřičná práva jednotlivým uživatelům pro přístup ke službám a datům. Je zde popsáno, které systémy budou monitorovat a zaznamenávat úspěšná a neúspěšná přihlášení.

  Kontroluje: Pracovník zajištující ochranu logického přístupu k datům

  Sankce: Za porušení navrhuji srazit zaměstnanci až 10000 Kč z pohyblivé složky mzdy.

4.6 Ochrana dat přenášených počítačovou sítí

Pracovníkovi, který má v popisu práce funkci pro ochranu dat přenášených počítačovou sítí, je umožněn přístup k záznamům navštěvovaných internetových stránek a je mu umožněno monitorování a testování sítě VPN a Wi-Fi.

Navrhuji vytvořit následující směrnici:

- **Směrnice o firemní komunikaci**

  Vytvoří: Pracovník zajišťující ochranu dat přenášených počítačovou sítí

  Popis: Směrnice popisuje práci s elektronickou poštou a chování zaměstnance na internetu a ve virtuální privátní síti VPN. Popisuje jaké zabezpečené protokoly a šifrování pro přenášení citlivých dat se ve firmě používají a jakým způsobem.

  Kontroluje: Pracovník zajišťující ochranu dat přenášených počítačovou sítí

  Sankce: Za nedodržení navrhuji srazit zaměstnanci až 5000 Kč z pohyblivé složky mzdy.

- **Směrnice o používání firemní bezdrátové sítě Wi-Fi**

  Vytvoří: Pracovník zajišťující ochranu dat přenášených počítačovou sítí

  Popis: Směrnice popisuje jaká zařízení je možno připojovat do bezdrátové sítě, komu je to umožněno a pravidla pro bezpečnou práci s bezdrátovou sítí.

  Kontroluje: Ředitel bezpečnosti

  Sankce: Za nedodržení navrhuji srazit zaměstnanci až 5000 Kč z pohyblivé složky mzdy.

4.7 Ochrana dat před zničením

Pracovníkovi, který má v popisu práce funkci pro zajištění ochrany dat před zničením, je poskytnuta veškerá dostupná dokumentace k zálohovacím zařízením a zálohovacím médiím využívaných ve firmě. Je mu poskytnut přístup do serverovny, k zálohovacím zařízením a systémům, které se zálohují.

Navrhuji vytvořit následující směrnice:

- **Směrnice o zálohování dat**

  Vytvoří: Pracovník zajišťující ochranu dat před zničením ve spolupráci s vlastníky dat

  Popis: Tato směrnice popisuje formy zálohování, které se ve firmě realizují. To znamená – co se zálohuje, na jaká média a jak často. Směrnice dále určuje kam ukládat data určená pro centralizované zálohování a jak zálohovat archivní data, která již není potřeba mít uložena na souborovém serveru.

  Kontroluje: Vedoucí oddělení, kterému data patří

  Sankce: Za nedodržení navrhuji srazit zaměstnanci až 5000 Kč z pohyblivé složky mzdy.

- **Směrnice o práci se záložními kopiemi dat**

  Vytvoří: Pracovník zajišťující ochranu dat před zničením

  Popis: Určuje do jaké vzdálené lokality se budou ukládat záložní kopie, jak často a kdo to bude provádět. Směrnice popisuje jak se chovat k jednotlivým typům záložních médií a s jakým prostředím by neměly přijít do styku. Je zde popsáno jakým způsobem je vedena evidence záložních kopií, kam budou ukládány a co má obsahovat identifikační popisek záložní kopie.

  Kontroluje: Ředitel bezpečnosti IT

  Sankce: Při nedodržení navrhuji srazit zaměstnanci až 10000 Kč z pohyblivé složky mzdy.

- **Směrnice: Havarijní plán a kontrola obnovy dat**

  Vytvoří: Pracovník zajišťující ochranu dat před zničením

  Popis: Tato směrnice popisuje co to jsou havarijní stavy a jak je řešit. Směrnice stanovuje: kdo je zodpovědný za krizové řízení, kdo a za jakých podmínek vyhlašuje havarijní stav, jaké kroky je třeba podniknout pro obnovu důležitých částí systému a ztracených dat pro jednotlivé druhy

havárií. Směrnice také obsahuje postup a frekvenci kontroly obnovení dat ze záloh. Administrativní část stanovuje kde budou havarijní plány rozmístěny a jak často podléhá havarijní plán revizi.

Kontroluje: Ředitel bezpečnosti IT

Sankce: Za nedodržení postupů uvedených v havarijním plánu navrhuji sankce do výše desetitisíců korun z pohyblivé složky mzdy.

4.8 Personální bezpečnost

Pracovníkovi, který má v popisu práce funkci pro personální bezpečnost, musí být poskytnut přehled o všech platných bezpečnostních směrnicích ve firmě, aby je mohl zohlednit ve směrnici o školení zaměstnanců. Dále je obeznámen s procesem přijímání a propouštění zaměstnanců ve firmě.

Navrhuji vytvořit následující směrnice:

- **Směrnice o zabezpečení přijetí do pracovního poměru**

  Vytvoří: Pracovník zajišťující personální bezpečnost ve spolupráci s hlavním personalistou

  Popis: Tato směrnice určuje jakým způsobem prověřit budoucího zaměstnance, aby mu mohl být přidělen přístup do IS. Je zde popsáno na základně jakých kritérií mu budou přiřazeny hesla, čipová karta nebo klíče a jakým způsobem a co bude oznámeno ostatním zaměstnancům, kterých se jeho nástup týká.

  Kontroluje: Hlavní personalista

  Sankce: Za nedodržení navrhuji srazit zaměstnanci až 10000 Kč z pohyblivé složky mzdy.

- **Směrnice o školení zaměstnanců o bezpečnosti IS/IT**

  Vytvoří: Pracovník zajišťující personální bezpečnost ve spolupráci s hlavním personalistou

Popis: V této směrnici je popsán obsah úvodního a dalších průběžných školení o bezpečnosti IS/IT ve firmě, kdo bude školit a jaké zaměstnance je potřeba proškolit na jaké směrnice.

Kontroluje: Hlavní personalista

Sankce: Sankce nejsou, jedná se o předpis

- **Směrnice o zabezpečení při rozvázání pracovního poměru**

  Vytvoří: Pracovník zajišťující personální bezpečnost ve spolupráci s hlavním personalistou

  Popis: Směrnice stanovuje povinnost personalisty informovat správce IT o ukončení pracovního poměru se zaměstnancem. Je zde popsáno jaká oprávnění je nutné odebrat při ukončení pracovního poměru (zrušení oprávnění v IS, zrušení e-mailové schránky, změna sdílených hesel, zrušení přístupu do VPN).

  Kontroluje: Ředitel bezpečnosti IT

  Sankce: Za nedodržení navrhuji srazit odpovědnému zaměstnanci až 10000 Kč z pohyblivé složky mzdy.

- **Směrnice o sankcích za narušení bezpečnosti IS/IT**

  Vytvoří: Pracovník zajišťující personální bezpečnost ve spolupráci s hlavním personalistou

  Popis: Tato směrnice stanovuje pravidla pro udělování sankcí, kdo o jejich udělování rozhoduje, jejich výši a postupy při opakovaném porušování směrnic a předpisů.

  Kontroluje: Jednatel

  Sankce: Nejsou

4.9 Ekonomické zhodnocení návrhu

V této části vyčíslím finanční náklady na navrhované řešení a uvedu jeho ekonomický přínos.

Směrnice budou vytvářet pracovníci od externího správce IT ve spolupráci se zaměstnanci firmy, od kterých budou získávat pokyny, informace a podpůrné materiály. V případě zaměstnanců firmy bude čas strávený na této spolupráci zahrnut do jejich běžné pracovní doby. Tvorba směrnic bude vyžadovat přítomnost pracovníků externího správce IT v centrální budově firmy za smluvní sazbu 790kč/hod bez DPH. Počet směrnic je 17 a průměrný čas strávený tvorbou jedné směrnice odhaduji na 2 hodiny.

Z toho vychází odhad ceny na tvorbu bezpečnostních směrnic:

$$17 \cdot 2 \cdot 790 = 26\,860\ \textit{Kč bez DPH}$$

Cena za vytvoření směrnic je orientační. Čas potřebný k tvorbě směrnic je pozitivně ovlivněn tím, že pracovníci externího správce IT jsou seznámeni s firemním IS, se zpracovávanými daty a chodem firmy.

Většina navrhovaných směrnic bude obsahovat bezpečnostní opatření administrativního nebo organizačního charakteru vyžadující minimální nebo nulové náklady. Tvůrci směrnic v nich ale mohou stanovit také bezpečnostní opatření, které vyžaduje významnou finanční investici. V tom případě bude potřeba provést konzultaci s vedením firmy a objasnit nutnost a možnosti implementace daného opatření. Vedení firmy bude rozhodovat o tom, zda se bezpečnostní opatření bude realizovat, nebo může vybrat levnější variantu řešení, která snižuje riziko na požadovanou úroveň.

Není cílem práce počítat výnosy (úspory) ze zavedení všech možných bezpečnostních opatření, které budou teprve určeny ve finálních směrnicích. Proto zde uvedu pouze příklad z minulosti zkoumané firmy z oblasti zabezpečení fyzického prostředí. V roce 2007 nastala ve firmě řada bezpečnostních incidentů způsobených příliš vysokou teplotou vzduchu v místnosti serverovny, která dosahovala až 35ºC. Riziko poškození hardware serverů a ztráty dat bylo vysoké. V důsledku přehřívání a následného poškození komponent serverů (pevné disky, zdroje) byly servery střídavě mimo provoz a chod firmy byl omezen. Přímé finanční náklady na nový hardware, obnovu dat a další práci techniků byly přibližně 90 tisíc korun. Po zavedení

bezpečnostního opatření ve formě klimatizace za 30 tisíc korun se podobné bezpečnostní incidenty již neopakovaly a riziko poškození hardware a ztráty dat v důsledku přehřívání je nyní velmi nízké. Z uvedeného příkladu je zřejmé, že bezpečnostnímu incidentu se dalo předejít vytvořením a respektováním směrnice, která by určovala požadované klimatické podmínky v místnosti serverovny.

Rentabilitu investice bude možné měřit s časovým odstupem a to tak, že bude srovnáván počet bezpečnostních incidentů a náklady na ně vynaložené před zavedením řízení bezpečnosti a po jeho zavedení. Mimo možné finanční úspory získává firma přidanou hodnotu v podobě větší produktivity práce, konkurenceschopnosti a věrohodnosti.

5 Závěr

V mé práci jsem se zabýval bezpečnostní politikou IS/IT reálné české firmy. Analytickou část jsem zaměřil na popis stavu informačních technologií ve firmě z pohledu ochrany dat a řízení bezpečnosti. Během analýzy jsem odhalil několik vážných nedostatků v současné bezpečnostní politice firmy.

V návrhu řešení jsem stanovil nový bezpečnostní cíl a strategii firmy. Z této strategie vychází navrhovaná organizační struktura pro bezpečnost IS/IT ve firmě. Jako součást návrhu řešení uvádím také návrhy na vytvoření bezpečnostních směrnic v oblastech fyzické bezpečnosti a bezpečnosti prostředí, klasifikace a ochrany uložených dat, ochrany logického přístupu k datům, ochrany dat přenášených počítačovou sítí, ochrany dat před zničením a personální bezpečnosti. Z ekonomického hlediska považuji zavedení řízení bezpečnosti ve firmě jako výhodnou dlouhodobou investici a domnívám se, že firmě nebude působit velikou finanční zátěž.

Je dobré si uvědomit, že kvalitní a fungující bezpečnostní politika významně snižuje podnikatelské riziko a představuje pro firmu konkurenční výhodu. Věřím, že mnou navržené řešení bude pro firmu přínosem a že otázky bezpečnosti IS/IT nebude firma podceňovat.

Literatura

Knižní publikace

[1] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Computer Press, 2005. ISBN 80-251-0574-1.

[2] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Computer Press, 2004. ISBN 80-251-0106-1.

[3] DOSTÁLEK, L. A KOL. *Veklý průvodce protokoly TCP/IP: Bezpečnost*. 2. vyd. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[4] HANÁČEK, P., STAUDEK, J. *Bezpečnost informačních systémů*. Praha: ÚSIS, 2000. 127 s. ISBN 80-238-5400-3.

[5] HORÁK, J. *Bezpečnost malých počítačových sítí*. Grada, 2003. ISBN 80-247-0663-6.

[6] PROSICE, C., MANDIA, K. *Počítačový útok: Detekce, obrana a okamžitá náprava*. Computer Press, 2002. ISBN 80-7226-682-9.

Internetové zdroje

[7] BITTO, O. *Jak jsou na tom s bezpečností organizace v ČR?* [online]. [cit. 10.4.2008]. Dostupný z: <http://www.lupa.cz/clanky/jak-jsou-na-tom-s-bezpecnosti-organizace-v-cr/>.

[8] BOUČEK M. *Ochrana osobních údajů* [online]. [cit. 20.4.2008]. Dostupný z: <http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju/1000818/7196/>.

[9] JANOUŠEK, M. *Kyberterorismus: Terorismus informační společnosti* [online]. [cit. 15.4.2008]. Dostupný z: <http://www.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf>.

[10] KUNDEROVÁ, L. *Bezpečnost IS: Snímky k přednáškám* [online]. [cit. 10.3.2008]. Dostupný z: <https://akela.mendelu.cz/~lidak/share/snimky-bis/>.

[11] STAUDEK, J. *Bezpečnost IT* [online]. [cit. 12.3.2008]. Dostupný z: <http://www.fi.muni.cz/usr/staudek/vyuka/security/PV017.xhtml>.

[12] YHAN, G. *ISO 17799: Scope and implementation – Part 1 Security Policy* [online]. [cit. 22.4.2008]. Dostupný z: <http://www.infosecwriters.com/text_resources/pdf/ISO17799.pdf.>.

[13] *Bezpečnost IS/IT* [online]. [cit. 20.4.2008]. Dostupný z: <http://www.itil.cz/index.php?id=1003>.

[14] *Bezpečnost IT* [online]. [cit. 16.3.2008]. Dostupný z: <http://www.gity.cz/cz/zakaznicka-reseni/bezpecnost-it/>.

[15] *Bezpečnostní politika* [online]. [cit. 16.3.2008]. Dostupný z: <http://www.gity.cz/cz/zakaznicka-reseni/bezpecnost-it/bezpecnostni-politka-cbp-sbp/>.

[16] *Confidentiality, integrity, availability (CIA)* [online]. [cit. 20.4.2008]. Dostupný z: <http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm>.

[17] *Implementace bezpečnostní legislativy* [online]. [cit. 30.4.2008]. Dostupný z: <http://www.logica.cz/implementace+bezpecnostn%C3%AD+legislativy/400007933>.

[18] *ISO/IEC 27001:2005* [online]. [cit. 30.4.2008]. Dostupný z: <http://www.rac.cz/rac/homepage.nsf/CZ/27001>.

[19] *Legislativa, Standardy, Metodiky* [online]. [cit. 15.4.2008]. Dostupný z: <http://www.tsoft.cz/index.php?q=cz/legislativa>.

Normy

[20] ČSN ISO/IEC TR 13335-1:1999. Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT. Praha: Český normalizační institut, 1999. 22s.

[21] ČSN ISO/IEC TR 13335-2:1999. Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 2: Řízení a plánování bezpečnosti IT. Praha: Český normalizační institut, 1999. 22s.

[22] ČSN ISO/IEC TR 13335-3:1999. Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 3: Techniky pro řízení bezpečnosti IT. Praha: Český normalizační institut, 1999. 45s.

[23] ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006. 35s.

[24] ISO/IEC 17799. Information technology – Security Techniques – Code of practice for information security management. International organization for standardization, 2005. 115s.

Zákony a vyhlášky

[25] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000.

Seznam obrázků a tabulek

Seznam příloh

Příloha 1: Doporučená klasifikace dat

Navrhované klasifikační třídy:

Úroveň 1: Veřejná/neutajovaná data – Do této kategorie spadají data, která jsou volně šířitelná anebo dostupná z volně šířitelných zdrojů. Nemají pro podnik zvláštní hodnotu a při jejich prozrazení nehrozí finanční nebo jiná ztráta

Úroveň 2: Interní data – Jedná se o vnitropodniková data, jejichž prozrazení může mít pro firmu minimální škodu s nepatrnými následky.

Úroveň 3: Důvěrná data – Jsou to vnitropodniková data, jejichž prozrazení může mít za následek poškození společnosti ve formě finanční ztráty, ztráty zákazníků a jejich důvěry, poskytnutí informací konkurenci, zhoršení pověsti společnosti, atd.

Úroveň 4: Tajná data – Zahrnuje kritická vnitropodniková data, jejichž prozrazení může vést k porušení zákonů, finanční ztrátě velkého rozsahu a platební neschopnosti, ztrátě pozice na trhu, hrubému poškození pověsti společnosti, atd.

Typy dat zjištěné při analýze ohodnocené podle navržené stupnice:

Typ dat	Úroveň
databáze firemního účetnictví (fakturace, majetek, platební styky, atd.)	4
databáze pro personalistiku a mzdy	4
dokumentace firemních plánů a strategií	4
databáze odběratelů a dodavatelů s údaji o jejich obchodní historii, slevách, kontaktech, smluvních podmínkách, atd.	4
databáze produktů firmy a technické listy	3
dokumenty interních podnikových směrnic a předpisů	3
dokumenty a analýzy o konkurenci	3

databáze elektronické pošty a do ní vložených souborů příloh	4
záznamy z kamerového systému	4
systémové zálohy	4
fotografie z akcí	2
volně šiřitelné dokumenty (reklamní materiály, obsah www stránek)	1